NATIONAL DEFENSE UNIVERSITY
STRATEGIC FORUM
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

Number 99, December 1996

Information Warfare

An Old Operational Concept With New Implications

by Abe Singer and Scott Rowell

Conclusions

- The new balance of information and energy (as well as the degree of coupling between them) is changing the conduct of warfare.

- Expect to see much more intensive use of deception, stealth and redundancy as well as much smaller and stealthier platforms in order to neutralize the impact of highly accurate PGMs. Taken in aggregate, these changes call for fundamentally different approaches to the design and development of weapon systems, which, in turn, will inevitably lead to basic changes in strategy, tactics and doctrine.

- Key assets of the national civilian infrastructure may, under certain circumstances, become highly lucrative military centers of gravity for an adversary, blurring the traditional dividing line between the combatant and civilian domains. Even more disturbing is the nature of this critical vulnerability-involving asymmetry of forces, arduous tracing of information warfare attacks, and the bypassing of the military.

- These conditions, and their interrelationships, may radically alter the role of the military as well as our definition of war.

A Fundamental Question

Information warfare has recently captured the attention of the news media. Numerous articles on the subject have appeared in the popular press-a cover story in Time, a major article in Scientific American, and many op-ed pieces in major newspapers. Yet information warfare is virtually as old as warfare itself. For example, Joshua used information warfare (as feigning tactics) three thousand four hundred years ago in the capture of 'Ay; the Greek city-states conducted information warfare (in the form of deception) two hundred years later in their conflict with Troy; and during the Absalom Rebellion three thousand years ago, King David succeeded in overloading Absalom's decision-making process with unnecessary information-precipitating the reversal of a critical military decision-thus saving David from virtually certain destruction and assuring ultimate victory.

So what's new about information warfare? Is it just the latest buzz word? Is it merely the consolidation

of a large set of incremental increases in the role of information in warfare during the last three decades-primarily in the areas of precision guided munitions (PGM) as well as in command, control, communications and intelligence-or is it the leading edge of a step-function change having enormous implications on how wars will be fought in the future? Many unbiased, analytical thinkers are skeptical about any dramatic change. Unfortunately, current literature on information warfare contributes to this skepticism.

An examination of the open literature on information warfare shows that recent attempts to address this issue suffer from two major shortcomings. Authors either (1) get involved in attempts to predict technology, thus incurring a loss of credibility with many readers (history is replete with examples of how technology predictions can make fools of some of the brightest minds), or (2) they wrap information warfare up in the broader issues of a revolution in military affairs, thereby losing focus and becoming diverted by irrelevant controversies. A radically different approach to the subject is obviously in order.

Energy and Information

In his book On the Psychology of Military Incompetence (published almost half a century ago), Brigadier General Norman Dixon makes this interesting observation: "War is primarily concerned with two sets of activities-the delivery of energy and the communication of information." In other words, in its most basic form, war boils down to two dimensions, energy and information. Drawing on Dixon's work, the 'information-energy' lens provides an excellent vehicle for addressing the issue of what's new about information warfare, because it allows us to maintain the same paradigm while examining warfare throughout human history-from the days of the caveman, to the agrarian age, to the invention of gunpowder, to the industrial age, to the information age. In this context, what has changed in warfare over the years is the magnitude and intensity of these two dimensions as well as the degree of coupling between them. The energy dimension comes into play in conventional warfare primarily in its kinetic mode-largely as steel delivered at high velocity. The information dimension, on the other hand, appears in numerous manifestations which usually fall into one of three categories-command and control, attacks on the opponent's information system, or leveraging of energy.

During most of recorded history, troops fought in relatively tight formations, largely driven by the limited firepower and range of their weapons. This considerably simplified the information dimension in combat. In the battle of Waterloo (18 June 1815), for example, Napoleon, mounted on horseback on a nearby hill, could observe the entire battlefield and direct his forces by means of couriers and personal presence. The turn of the century saw a dramatic increase in the firepower and range of conventional weapons, countered by a corresponding increase in dispersion made possible by significant enhancements in command and control. The outcome of the vast majority of battles, however, continued to be determined by energy considerations because the technology for effectively leveraging energy by information was as yet unavailable. Thus, according to Lt. Gen. James Clapper, former head of the Defense Intelligence Agency, as late as 1943 during World War II it took 9,000 2000-lb bombs dropped by 1,500 B-17 sorties to destroy a 60Ox100O target. A quarter of a century afterwards, in 1970 in Viet Nam, it took 176 such bombs and 88 F-4 sorties. But a mere 20 years later, in 1991 during DESERT STORM, it took only one or two laser-guided bombs in conjunction with a single F-117 sortie. The energy-information equation has been changing drastically during the last three decades. And the change is being driven primarily by a single agent: solid state electronics.

Solid State Electronics

All technological revolutions of this century pale in comparison with the spectacular revolution in solid

state electronics over the last three decades-the likes of which has never been seen before in human history. This in turn has generated a comparable phenomenal revolution in information. Today we can process vast amounts of information almost instantaneously, at extremely low cost. We can then transmit that information in virtually no time with very high reliability to any point on the globe almost for free. To see this in proper perspective, it is useful to use an analogy from a high-tech industry. If the aircraft industry, for example, had undergone similar progress during the last three decades, a trip from Tokyo to Washington, D.C., would take less than five minutes, would cost $2, and would all be done on less than half a gallon of gas.

Role of Platforms in a PGM Environment

The coupling between energy and information in a projectile degrades with distance and time of flight unless it is somehow reinforced. For instance, a tiny angular error in the velocity vector of a projectile translates into a larger and larger linear error the further the projectile travels. Guidance systems accumulate errors with time and distance due to drifts in the reference as well as due to errors incurred in compensating for forces encountered in flight. Sometimes, when the distance to the target is very large, the offense may not be able to deliver energy with sufficient lethality to make the process cost effective. At other times, the distance may be so large that the offense may simply not be able to deliver the energy at all. This is where platforms come in-e.g., aircraft, ships, aircraft carriers, etc.

While a platform has many functions, e.g., to intimidate an enemy, to show the flag to friend and foe, its most fundamental function is to shorten the distance between the launching point and the target, so that energy can be delivered to the target with enough lethality to make the attack cost effective. However, the closer a platform comes to the target, the more vulnerable it becomes and the more assets it consumes not only to get there, but, perhaps more importantly, for self-protection.

But when PGMs can hit a target hundreds of miles away with a single-shot kill probability close to one, it is time to re-examine the fundamental role of key weapon systems-particularly large platforms-in terms of their cost-effectiveness in combat. For example, how many precision guided missiles does it take to overwhelm the defenses of a particular platform? What percentage of missiles need to get through? How much damage does such an attack have to inflict on the platform in order to put it out of commission for, say, several hours? What is the cost of inflicting such damage? How does it compare with the cost of defending against it? How does it compare with the cost of sustaining and repairing the damage? In other words, what is the cost-exchange ratio?

In a recent test of the potential vulnerability of a carrier task force, the task force successfully defended itself against 20 simulated cruise missiles attacking it simultaneously. How realistic was the simulation? Specifically, how well did the simulation represent the threat? How comprehensive was it? What would the outcome have been with 30 attacking missiles? With 40?

The analytical tools for comprehensively addressing these questions are not yet available. Virtually all existing combat simulations play primarily the energy dimensions of warfare, with the other parameters, especially information, appearing in the background as force multipliers or just taken for granted. These simulations will have to be discarded, and new models explicitly incorporating the information dimension will have to be designed and tested. They will undoubtedly show, as General Gordon Sullivan recently noted, that although the nature of war has not changed, the conduct of war is changing dramatically.

Consequently, the roles of many key assets in combat must be re-examined. For example, cost

operational effectiveness analyses, based on such new simulations, are likely to show that it makes more sense to go to much smaller and stealthier platforms, deployed in significantly different ways. (As an immediate side benefit here, the concern about the exponential cost growth of large platforms-an issue that has bedeviled military planners during the last few decades-may significantly decline in importance.) In addition we are likely to see a much more intensive use of deception and stealth as well as redundancy of critical assets in order to neutralize the impact of PGMs. Battle damage assessment will therefore be much more difficult to achieve successfully. Very low cost information processing makes encryption of digital communications much more cost effective than code breaking. Communications in combat will therefore be considerably more secure, particularly at higher levels (e.g., Division & Corps). The new simulations are also likely to show that information sharing among the military services will be crucial. For example, the Air Force would provide Intelligence, Surveillance and Target Acquisition (ISTA) support to the Army by means of small low-earth-orbiting satellites that can be readily launched from aircraft (e.g., Pegasus). (Large satellites would be too vulnerable for combat use.) And the Army would augment that support by heavy use of remotely piloted vehicles and light, solar powered gliders.

These changes call for fundamentally different approaches to the design and development of weapon systems. And this, in turn, will inevitably lead to basic changes in strategy, tactics and doctrine. In short, we are on the threshold of a radically different approach to military affairs.

A New Soft Dimension

The modern military relies very heavily on processing and transmission of vast amounts of information-and consequently is highly vulnerable to exploitation in this area. This vulnerability is rising sharply as we move further and further into the information age. And this is to be expected. A new critical vulnerability, however, has recently emerged.

As a result of the phenomenal revolution in solid state electronics and consequent cataclysm in information processing and transmission, some key national civilian institutions have drastically altered their modes of operation. Some examples of such institutions include banking, stock markets, telephone switching networks, electric power grids, and air traffic control systems. They increasingly rely on information to significantly improve their efficiency in order to survive in fiercely competitive markets. The flip side of this efficiency is that these assets have become the soft underbelly of the nation, with significant implications for national security. Even a partially successful attack on any one of these targets could have devastating economic consequences. This blurs the traditional dividing line between the combatant and civilian domains.

While considerable disagreement exists among experts as to how difficult it would be to execute such an attack by purely electronic means, many believe that it could be implemented with relative ease when coupled with human intelligence (HUMINT). If one were to define an act of war in terms of damage inflicted, rather than in the traditional Clausewitzian terms (which focus on the intent of the attacking nation and the means used for carrying out the attack) on which our current defense laws are based, then such attacks on the national infrastructure would certainly be classified as warfare.

Increased vulnerability is, however, only part of the problem. What is more disturbing is the nature of the vulnerability. A mere handful of the "right" people, working in conjunction with the appropriate HUMINT, could inflict enormous damage on a nation by bringing down a key segment of its infrastructure. And, they can do it while working outside the country, in the safety of an office thousands of miles away, at times leaving no "fingerprints."

If an outside enemy were to try to inflict such damage by traditional physical means, the military would quickly come to the defense of such national institutions. What is the role of the military when the attack is implemented by electronic means? How would we ascertain, with a high degree of confidence, the location of the attacker? If the attack came from another country, what was the degree of involvement on the part of its government? How do we go about proving it? Can we hold that government responsible? How do we retaliate? We may have to drastically change not only the function of the military but also our definition of war.

To quote General Giulio Douhet, a leader in a revolution in military affairs during an earlier age, "Victory smiles upon those who anticipate changes in the character of war, not upon those who wait to adapt themselves after the changes occur." " And considering the nature of changes we are facing-from the very painful and tangible (lethality) to the tormenting but intangible (information)"it might be worth recalling the words of Thomas Sowell: "It takes a vision to beat a vision."

Dr. Abe Singer is a professor at the Industrial College of the Armed Forces, National Defense University; he can be reached at (202) 685-4375 or through the Internet at singera@ndu.edu. Colonel Scott Rowell, USA, is a Military Assistant to the Director of Net Assessment, Office of the Secretary of Defense; he can be reached at (703) 697-1312 or through the Internet at rowells@policy1.policy.osd.mil.

|Return to Top | Return to Strategic Forum Index |Return to Research and Publications|

The Strategic Forum provides summaries of work by members and guests of the Institute for National Strategic Studies and the National Defense University faculty. These include reports of original research, synopses of seminars and conferences, the results of unclassified war games, and digests of remarks by distinguished speakers.

Editor in Chief - Hans Binnendijk

Editor - Jonathan W. Pierce

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Information Warfare: An Old Operational Concept with New Implications

B. DATE Report Downloaded From the Internet: 09/27/01

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **National Defense University Press**
Institute for National Strategic Studies
Washington, DC 20001

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 09/27/01**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.